证　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：2002 09 30

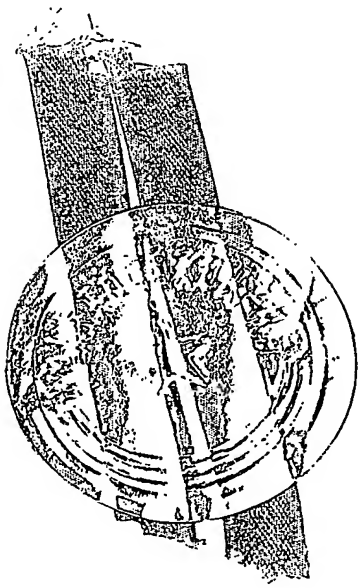
申　请　号：02 1 44083.2

申请类别：发明

发明创造名称：多媒体广播与组播业务中密码的管理及分发方法

申　请　人：北京三星通信技术研究有限公司；三星电子株式会社

发明人或设计人：朱彦民



中华人民共和国
国家知识产权局局长 王景川

2003 年 10 月 22 日

权 利 要 求 书

1. 一种多媒体广播与组播业务中密码的管理及分发方法，包括步骤：

组密码位于最高层的根节点，所述根节点只有子节点没有父节点；

对应用户的私人密码位于叶节点，所述叶节点是MBMS服务的用户；

中间节点具有本身的密码，所述中间节点拥有一个父节点和一个或多个子节点。

2. 按权利要求1所述的方法，其特征在于所述每个用户保存着从各自所处的叶节点到树的根节点的节点链所经过的包括叶节点、中间节点和根节点在内的所有节点的节点密码信息。

3. 按权利要求1所述的方法，其特征在于当一个新用户加入MBMS服务时，该用户被作为一个新叶节点通过其接入父节点连到树上，这个用户要获得从其接入父节点到树的根节点的节点链所经过的中间节点和根节点在内的所有节点的节点密码，这些节点密码不因为该用户的加入而发生更新，这些节点密码的传递依次通过点到点的方式发送给该用户并利用该新叶节点密码进行加密。

4. 按权利要求1所述的方法，其特征在于当一个新用户加入MBMS服务时，该用户被作为一个新叶节点通过其接入父节点连到树上，这个用户要获得从其接入父节点到树的根节点的节点链所经过的中间节点和根节点在内的所有节点的节点密码，这些节点密码因为该用户的加入而发生更新，对这个新加入的用户而言，这些新的节点密码的传递依次通过点到点的方式发送给该用户并利用该新叶节点密码进行加密。

5. 按权利要求4所述的方法，其特征在于，对于所述需要更新密码的每一个节点，新密码将利用旧密码进行加密并通过点到多点播送的方式传递给各自所属的最终叶节点用户。

6. 按权利要求1所述的方法，其特征在于当一个用户离开MBMS业务时，其叶节点从其父节点断开，从该断开节点到树的根节点的节点链所经过的所有节点的节点密码依次进行更新。

7. 按权利要求6所述的方法，其特征在于对于所述需要更新密码的每一个节点，节点密码的更新等到其所有子节点密码更新完成后进行。

8. 按权利要求6所述的方法，其特征在于对于所述需要更新密码的每一个节点，新的节点密码通过点到点的方式逐个传送给其所有子节点，并采用各子节点的密码分别进行加密。

9. 按权利要求8所述的方法，其特征在于所述各子节点依然采用其对应的节点密码对所述新的节点密码进行加密，并通过点到多点播送的方式传递给各自所属的最终叶节点用户。

10. 按权利要求1所述的方法，其特征在于所述信息加密过程由RNC完成。

11. 按权利要求1所述的方法，其特征在于所述根节点与中间节点共同位于同一个逻辑网络设备。

12. 按权利要求1所述的方法，其特征在于所述根节点与中间节点位于不同的逻辑网络设备。

说　　明　　书

多媒体广播与组播业务中密码的管理及分发方法

技术领域

本发明涉及多媒体广播与组播业务（以下简称MBMS），特别是涉及多媒体广播与组播业务中密码的管理及分发方法。

背景技术

MBMS是在第三代移动通信系统合作伙伴计划中正在为之制定相关标准以进行标准化的一项新业务。MBMS业务是一种单向的点到多点方式（即从单一数据源播发出多媒体数据经过网络传输被送到多个用户接收）的业务。这种业务的最大特点是它可以有效的利用无线资源和网络资源。MBMS业务主要用于无线通信网络系统中，如宽带码分多址通信系统，全球移动通信系统等。MBMS中业务数据的发送基本上要经过：数据源发送、中间网络传输、目的小区空中传输、用户接收这样几个过程。图16是一个能够提供MBMS业务的无线通信系统逻辑网络设备图，在该图中MBMS实际上利用了通用分组无线数据业务（以下简称GPRS）网络作为核心传输网络。如图16所示，广播及组播服务中心（以下简称BM-SC）是发送MBMS业务数据的数据源；网关GPRS支持节点（以下简称GGSN）用于GRPS网络与外部网络（如INTERNET网络）的连接；在MBMS业务中网关GPRS支持节点连接BM-SC并把MBMS数据发送到特定的服务GPRS支持节点（以下简称SGSN）；小区广播中心是小区广播的数据源，在MBMS中通过将小区广播中心与BM-SC互连，使小区广播中心可以提供MBMS业务宣告功能；SGSN用于对UE进行接入控制及移动管理同时把从GGSN来的MBMS数据发送到特定的无线单元控制器（以下简称RNC）中去；　RNC用于控制一组基站并把多媒体数据传送到特定的基站中去；基站在RNC的控制下为某个小区的MBMS业务建立空中物理信道；终端用户设备（以下简称UE）是接收MBMS数据的终端设备。

图17中给出了MBMS业务从业务宣告、用户加入、业务通知、无线承载建立到最后用户离开的全部过程。

000 订阅建立起用户和服务提供商之间的联系，授权用户可以接收有关的MBMS服务。

001 业务宣告通知用户将要提供的MBMS业务。例如，系统要在下午7：00在北京市区转播一场足球赛。

002 加入表示用户加入一个组，即用户告诉网络他或她愿意接收这项组播业务。

003 MBMS组播承载建立为MBMS数据传输建立网络资源。

004 MBMS通知告知用户马上要进行的MBMS数据传输。

005 数据传输表示MBMS业务数据传输到用户的过程。

006 MBMS组播承载释放表示当MBMS业务数据传输完成后，释放网络资源。

007 离开与002 加入相对应，表示用户要离开一个组，即不再想接收某个业务的数据。

在一个无线通信网络系统中，一个用户和网络系统之间的信息交换要经过传输信道完成。无线通信网络系统中的传输信道一般有两种类型：单个用户独自占有的专用信道或者由多个用户共享的公用信道。一般而言，点到点（即从一个数据源发出的数据经过网络传输被送到一个用户接收）方式的传输通过专用信道完成，而点到多点的方式的传输通过公用信道来完成。通常情况下，为了保证在一个用户独自占有的专用信道上传递的数据的安全性，每个接入到无线通信网络系统中的用户都拥有一个只有该用户自己和网络系统知道的私人密码；用户和网络系统之间在专用信道上进行的数据传输利用该私人密码进行加密。而公用信道由于有多个用户共享，在公用信道上进行的数据传输一般不进行加密。为了有效地利用无线资源和网络资源，MBMS业务数据传输可以通过公用信道进行。这时，出于计费和安全等方面的考虑，MBMS业务数据通过公用信道传输时一般都要进行加密，以保证数据仅仅对那些可以接收的用户有意义。因此，接收MBMS服务的用户除了有自己的私人密码以外还需要知道MBMS服务组密码。

由于MBMS是一种点到多点的业务，为了有效地利用无线资源和网络资源，对位于一定服务范围内的所有正在接收同一种MBMS服务的一组用户来讲，MBMS业务数据加密所用的组密码应该是一样的。这样，用户就不必因为在此MBMS业务的服务范围内移动而更换不同的组密码。但在很多情况下，这个组密码应该经常进行更新。例如，当一个用户不再接收当前的MBMS服务而主动离开时，或者网络因计费等原因认为此用户不应该再接受当前的MBMS服务而使其被动离开时，为了避免此用户仍然可以利用旧的组密码而继续接收MBMS服务，组密码就需要进行更新并通知到组里的其他所有用户。

在现有的系统中，组密码的分发通常可以通过两种方式进行：针对每个用户通过点到点的传送方式逐个进行或者针对所有用户通过点到多点广播的方式进行。在通过点到点的方式逐个进行时，对MBMS业务组里面的每一个用户而言，组密码的传输都是用其对应的私人密码进行加密，这样就可以保证传给本用户的信息不被其他用户利用。在组的成员非常多并且成员经常变化时，由于对每次密码更新过程系统都需要通过点到点的方式逐个通知到组内成员，这种方式会给系统带来非常大的负载，完成一次组密码更新需要很长时间，效率很低。而在针对所有用户通过点到多点广播的方式进行时，新的组密码利用旧的组密码进行加密并进行广播发送；用户通过利用旧的组密码进行解密来获得新的组密码。由于已经离开了MBMS服务的用户依然可能保存着旧的组密码，此用户就有可能通过利用旧的组密码进行解密来获得新的组密码。因此，这种点到多点广播的密码分发方式存在密码泄露的不安全问题。

发明内容

因此，本发明的目的是提供一种适用于MBMS业务的安全高效的可以降低系统负载减少花费时间的密码管理和分发方法。

为实现上述目的，一种多媒体广播与组播业务中密码的管理及分发方法，包括步骤：

组密码位于最高层的根节点，所述根节点只有子节点没有父节点；

对应用户的私人密码位于叶节点，所述叶节点是MBMS服务的用户；

中间节点具有本身的密码，所述中间节点拥有一个父节点和一个或多个子节点。

本发明通过在一次密码更新过程中采用点到点方式和点到多点方式相结合的方法；同只采用点到点方式的密码更新方法相比，这种方法可以减少所需要的信息传递次数，降低了系统的负载并减少一次密码更新过程所需要的时间。而同只采用点到多点方式的密码更新方法相比，这种方法又解决了密码泄漏的安全性问题。

附图说明

图1是MBMS组的密码分配逻辑结构图；

图2是应用了本发明的第一个实施例的密码分配管理和逻辑网络设备图；

图3是与图2相应的当一个新用户加入MBMS服务并没有引起其他节点密码更新时的密码更新分发示意图；

图4是与图3相对应的流程图；

图5是与图2相应的当一个新用户加入MBMS服务并引起其他节点密码更新时的密码更新分发示意图；

图6是与图5相对应的流程图；

图7是与图2相应的当一个用户离开MBMS服务时的密码更新分发示意图；

图8是与图7相对应的流程图；

图9是应用了本发明的第二个实施例的密码分配管理和逻辑网络设备图；

图10是与图9相应的当一个新用户加入MBMS服务并没有引起其他节点密码更新时的密码更新分发示意图；

图11是与图10相对应的流程图；

图12是与图9相应的当一个新用户加入MBMS服务并引起其他节点密码更新时的密码更新分发示意图；

图13是与图12相对应的流程图；

图14是与图9相应的当一个用户离开MBMS服务时的密码更新分发示意图；

图15是与图14相对应的流程图；

图16是MBMS业务的无线通信系统逻辑网络设备图；

图17是MBMS组播业务流程图。

具体实施方式

本发明提供了一种适用于MBMS业务的安全高效的可以降低系统负载减少花费时间的密码管理和分发方法。它在一次密码分发过程中采用了点到点方式和点到多点方式相结合的方法。图1给出了MBMS组的密码分配逻辑结构图。密码的分配采用从根节点、各中间节点到叶节点的多层树状结构的排列，位于最底层的叶节点只有父节点没有子节点；中间节点可以拥有一到多个子节点，但是只能拥有一个父节点；位于最高层的根节点只有子节点没有父节点。不同的节点处有不同的节点密码。MBMS服务用户被分配位于各个叶节点上，叶节点密码即各个用户对应的私人密码，根节点密码即组密码。每个用户保存着从各自所处的叶节点到树的根节点的节点链所经过的包括叶节点、各层中间节点和根节点在内的所有节点的节点密码信息。MBMS业务数据采用根节点密码进行加密并播送到各个用户。

按照发明的一方面，新加入MBMS服务的用户被作为一个新叶节点通过其接入父节点连到树上。这个用户要获得从其接入父节点到树的根节点的节点链所经过的各层中间节点和根节点在内的所有节点的节点密码，这些节点密码不因为该用户的加入而发生更新。这些节点密码的传递通过点到点的方式发送给该用户并利用该新叶节点密码（即该用户的私人密码）进行加密。

按照发明的另一方面，新加入MBMS服务的用户被作为一个新叶节点通过其接入父节点连到树上。这个用户要获得从其接入父节点到树的根节点的节点链所经过的各层中间节点和根节点在内的所有节点的节点密码，这些节点密码因为该用户的加入而发生更新。对这个新加入的用户而言，这些新的节点密码的传递通过点到点的方式发送给该用户并利用该新叶节点密码（即该用户的私人密码）进行加密。另外，对这些节点中的每一个节

点而言，新密码还将利用旧密码进行加密并通过点到多点播送的方式传递给各自所属的最终叶节点用户。

按照发明的另一方面，当一个用户离开MBMS业务时，其叶节点被从其断开父节点脱离。从此断开节点到树的根节点的节点链所经过的所有节点的节点密码依次进行更新。对需要更新密码的每一个节点而言，父节点密码的更新等到其子节点密码更新完成后进行；新的父节点密码通过点到点的方式逐个传送给其所有子节点(脱离的叶节点除外)，并采用各子节点的密码分别进行加密；而各子节点通过点到多点播送的方式将其传递给各自所属的最终叶节点用户。

实施例

本专利涉及一种适用于MBMS业务的密码管理和分发方法；实际上，它通过在一次密码分发过程中采用点到点方式和点到多点方式相结合的方法来进行密码管理和分发，从而达到安全高效同时又可以降低系统负载减少花费时间的目的。参照所附图纸，下面给出了本发明的两个不同的实施例。为了避免使本专利的描述过于冗长，在下面的说明中，略去了对公众熟知的功能或者装置等的详细描述。

第一实施例

图2是应用了本发明的第一个实施例的密码分配管理和逻辑网络设备图。在这个实施例中，各节点密码的管理是由不同的逻辑网络设备完成，信息加密过程由RNC完成。图3是相应的当一个新用户加入MBMS服务并没有引起其他节点密码更新时的密码更新分发示图。图4是与图3相对应的流程图。图5是相应的当一个新用户加入MBMS服务并引起其他节点密码更新时的密码更新分发示意图。图6是与图5相对应的流程图。图7是相应的当一个用户离开MBMS服务时的密码更新分发示意图。图8是与图7相对应的流程图。

参照图2，一个BM_SC下面连接到若干个GGSN并为这些GGSN提供服务。每个GGSN下面又分别连接到若干个SGSN并为这些SGSN提供服务。每个SGSN下面又分别连接到若干个RNC并为这些RNC提供服务。每个

RNC又可以同时为若干个终端用户UE提供服务。图中的实线表示出了这些逻辑网络设备实体之间的连接。

在此BM_SC服务范围内的所有用户被视为一个MBMS服务组，组内的密码分配被分为三层。BM_SC作为根节点，其根节点密码Ko即为组密码。一个RNC下面的所有用户被分为若干个子组，每个子组即对应一个中间节点。例如，RNC11管理着若干个中间节点111，112…并分别为之分配节点密码K_{111}，K_{112}，…。每个终端用户作为一个叶节点，叶节点即为用户的私人密码。例如，终端用户1111的叶节点密码为K_{1111}，终端用户1121的叶节点密码为K_{1121}。图中的虚线表示出了这些逻辑密码节点之间的连接。每个终端用户保存着从各自所处的叶节点到树的根节点的节点链所经过的包括叶节点、各层中间节点和根节点在内的所有节点的节点密码信息。例如，终端用户1111保存着密码K_{1111}，K_{111}和Ko，终端用户1112保存着密码K_{1112}，K_{111}和Ko,终端用户1121保存着密码K_{1121}，K_{112}和Ko，终端用户1211保存着密码K_{1211}，K_{121}和Ko 。MBMS业务数据采用根节点密码Ko进行加密并播送。

参照图3到图4，无线通信网络系统为某终端用户1110分配的私人密码是K_{1110}。此终端用户希望接收当前BM_SC的MBMS服务，它通过“激活MBMS上下文请求”消息向SGSN1发出请求。无线通信网络系统进行一系列的操作后，接受了此请求。此用户被作为一个新叶节点1110通过其接入父节点111连到树上。这个用户要获得其接入父节点111的节点密码K_{111}和根节点的的节点密码Ko，密码K_{111}和Ko没有因为该用户的加入而发生更新。密码K_{111}和Ko作为“MBMS密码指配”消息的参数，被通过点到点的方式由RNC11在只有该用户使用的专用信道上发送给该用户。在这个只有该用户使用的专用信道上传递的信息，包括“MBMS密码指配”消息，利用该用户叶节点密码K_{1110}（即该用户的私人密码）进行加密。

参照图5到图6，无线通信网络系统为某终端用户1110分配的私人密码是K_{1110}。此终端用户希望接收当前BM_SC的MBMS服务，它通过“激活MBMS上下文请求”消息向SGSN1发出请求。无线通信网络系统进行一系列的操作后，接受了此请求。此用户被作为一个新叶节点1110通过其接入父节点111连到树上。这个用户要获得其接入父节点111的节点密码K_{111}和

根节点的的节点密码Ko，密码K_{111}和Ko因为该用户的加入而分别发生更新为新密码K_{111}'和Ko'。密码K_{111}'和Ko' 作为“MBMS密码指配”消息的参数，被通过点到点的方式由RNC11在只有该用户使用的专用信道上发送给该用户。在这个只有该用户使用的专用信道上传递的信息，包括“MBMS密码指配”消息，利用该用户叶节点密码K_{1110}（即该用户的私人密码）进行加密。

另外，新密码K_{111}'通过点到多点播送的方式通知到与终端用户1110处在同一个父节点111下面的其它所有叶节点用户1111，1112，1113……。新密码K_{111}'作为“MBMS密码指配”消息的参数，被通过点到多点播送的方式由RNC11在公用信道上传递给最终叶节点用户。这条“MBMS密码指配”消息被RNC11利用旧密码K_{111}进行加密。

另外，新根节点密码为Ko' 通过点到多点播送的方式通知到与终端用户1110处在同一个根节点BM_SC下面的其它所有叶节点用户。新密码Ko'被作为参数包含在“MBMS组密码变更请求”消息中从BM_SC通过GGSN传给各SGSN, SGSN将其作为参数包含在“无线接入承载指配请求”消息中从SGSN传给对应的各个RNC。然后，新密码Ko'作为“MBMS密码指配”消息的参数，被通过点到多点播送的方式由各RNC在公用信道上传递给最终叶节点用户。这条“MBMS密码指配”消息被各RNC利用旧密码Ko进行加密。

参照图7到图8，无线通信网络系统为某终端用户1110分配的私人密码是K_{1110}。此终端用户选择离开当前BM_SC的MBMS服务，它通过“去活MBMS上下文请求”消息通过RNC11向SGSN1发出请求。无线通信网络系统进行一系列的操作后，接受了此请求。其叶节点1110被从其断开父节点111脱离。断开节点111和根节点BM_SC的节点密码K_{111}和Ko依次更新为新密码K_{111}'和Ko'， Ko的更新等到K_{111}更新完成后进行。新密码K_{111}'作为“MBMS密码指配”消息的参数，被通过点到点的方式由RNC11在各个用户的专用信道上依次传递到与终端用户1110处在同一个父节点111下面的其它所有叶节点用户1111，1112，1113……。在每个用户的专用信道上传递的信息，利用该用户的叶节点密码（即该用户的私人密码）进行加密。新密码Ko'被作为参数包含在“MBMS组密码变更请求”消息中从BM_SC通过GGSN传给各SGSN, SGSN将其作为参数包含在“无线接入承载指配请求”消

息中从SGSN传给对应的各个RNC。然后，新密码Ko'作为“MBMS密码指配”消息的参数，被通过点到多点播送的方式由各RNC在公用信道上依次传递给各中间节点的最终叶节点用户。“MBMS密码指配”消息内容被各RNC利用对应的中间节点密码K_{111}'， K_{112}…，K_{121} …，K_{211}…分别进行加密。

第二实施例

图9是应用了本发明的第二个实施例的密码分配管理和逻辑网络设备图。在这个实施例中，各节点密码的管理是由同一个逻辑网络设备完成，信息加密过程由RNC完成。图10是相应的当一个新用户加入MBMS服务并没有引起其他节点密码更新时的密码更新分发示意图。图11是与图10相对应的流程图。图12是相应的当一个新用户加入MBMS服务并引起其他节点密码更新时的密码更新分发示意图。图13是与图12相对应的流程图。图14是相应的当一个用户离开MBMS服务时的密码更新分发示意图。图15是与图14相对应的流程图。

参照图9，一个BM_SC下面连接到若干个GGSN并为这些GGSN提供服务。每个GGSN下面又分别连接到若干个SGSN并为这些SGSN提供服务。每个SGSN下面又分别连接到若干个RNC并为这些RNC提供服务。每个RNC又可以同时为若干个终端用户UE提供服务。图中的实线表示出了这些逻辑网络设备实体之间的连接。

在一个RNC服务范围内的所有用户被视为一个MBMS服务组，组内的密码分配被分为三层。RNC作为根节点，其根节点密码即为组密码。RNC下面的所有用户被分为若干个子组，每个子组即对应一个中间节点。例如，RNC11根节点密码为Ko，它管理着若干个中间节点111，112…并分别为之分配节点密码K_{111}，K_{112}，…。每个终端用户作为一个叶节点，叶节点即为用户的私人密码。例如，终端用户1111的叶节点密码为K_{1111}，终端用户1121的叶节点密码为K_{1121}。图中的虚线表示出了这些逻辑密码节点之间的连接。每个终端用户保存着从各自所处的叶节点到树的根节点的节点链所经过的包括叶节点、各层中间节点和根节点在内的所有节点的节点密码信息。例如，终端用户1111保存着密码K_{1111}，K_{111}和Ko，终端用户1112保存着密码K_{1112}，K_{111}和Ko，终端用户1121保存着密码K_{1121}，K_{112}和Ko,终端

用户1211保存着密码K_{1211}，K_{121}和Ko 。MBMS业务数据采用根节点密码Ko进行加密并播送。

参照图10到图11，无线通信网络系统为某终端用户1110分配的私人密码是K_{1110}。此终端用户希望接收当前BM_SC的MBMS服务，它通过“激活MBMS上下文请求”消息向SGSN1发出请求。无线通信网络系统进行一系列的操作后，接受了此请求。此用户被作为一个新叶节点1110通过其接入父节点111连到树上。这个用户要获得其接入父节点111的节点密码K_{111}和根节点的的节点密码Ko，密码K_{111}和Ko没有因为该用户的加入而发生更新。密码K_{111}和Ko作为“MBMS密码指配”消息的参数，被通过点到点的方式由RNC11在只有该用户使用的专用信道上发送给该用户。在这个只有该用户使用的专用信道上传递的信息，包括“MBMS密码指配”消息，利用该用户叶节点密码K_{1110}（即该用户的私人密码）进行加密。

参照图12到图13，无线通信网络系统为某终端用户1110分配的私人密码是K_{1110}。此终端用户希望接收当前BM_SC的MBMS服务，它通过“激活MBMS上下文请求”消息向SGSN1发出请求。无线通信网络系统进行一系列的操作后，接受了此请求。此用户被作为一个新叶节点1110通过其接入父节点111连到树上。这个用户要获得其接入父节点111的节点密码K_{111}和根节点的的节点密码Ko，密码K_{111}和Ko因为该用户的加入而分别发生更新为新密码K_{111}’和Ko’。密码K_{111}’和Ko’ 作为“MBMS密码指配”消息的参数，被通过点到点的方式由RNC11在只有该用户使用的专用信道上发送给该用户。在这个只有该用户使用的专用信道上传递的信息，包括“MBMS密码指配”消息，利用该用户叶节点密码K_{1110}（即该用户的私人密码）进行加密。

另外，新密码K_{111}’通过点到多点播送的方式通知到与终端用户1110处在同一个父节点111下面的其它所有叶节点用户1111，1112，1113……。新密码K_{111}’作为“MBMS密码指配”消息的参数，被通过点到多点播送的方式由RNC11在公用信道上传递给最终叶节点用户。这条“MBMS密码指配”消息内容被RNC11利用旧密码K_{111}进行加密。

另外，新根节点密码为Ko’ 通过点到多点播送的方式通知到与终端用户1110处在同一个根节点RNC11下面的其它所有叶节点用户。新密码Ko’作

为“MBMS密码指配”消息的参数，被通过点到多点播送的方式由RNC11在公用信道上传递给最终叶节点用户。这条“MBMS密码指配”消息内容被RNC11利用旧密码Ko进行加密。

参照图14到图15，无线通信网络系统为某终端用户1110分配的私人密码是K_{1110}。此终端用户选择离开当前BM_SC的MBMS服务，它通过“去活MBMS上下文请求”消息通过RNC11向SGSN11发出请求。无线通信网络系统进行一系列的操作后，接受了此请求。其叶节点1110被从其断开父节点111脱离。断开节点111和根节点RNC11的节点密码K_{111}和Ko依次更新为新密码K_{111}'和Ko'， Ko的更新等到K_{111}更新完成后进行。新密码K_{111}'作为“MBMS密码指配”消息的参数，被通过点到点的方式由RNC11在各个用户的专用信道上依次传递到与终端用户1110处在同一个父节点111下面的其它所有叶节点用户1111，1112，1113……。在每个用户的专用信道上传递的信息，利用该用户的叶节点密码（即该用户的私人密码）进行加密。新密码Ko'作为“MBMS密码指配”消息的参数，被分别传递给各中间接点并由各中间接点通过RNC11利用点到多点播送的方式在公用信道上传递给对应的最终叶节点用户。这些“MBMS密码指配”消息内容被RNC11分别利用中间节点密码K_{111}'， K_{112}…，进行加密。

说 明 书 附 图

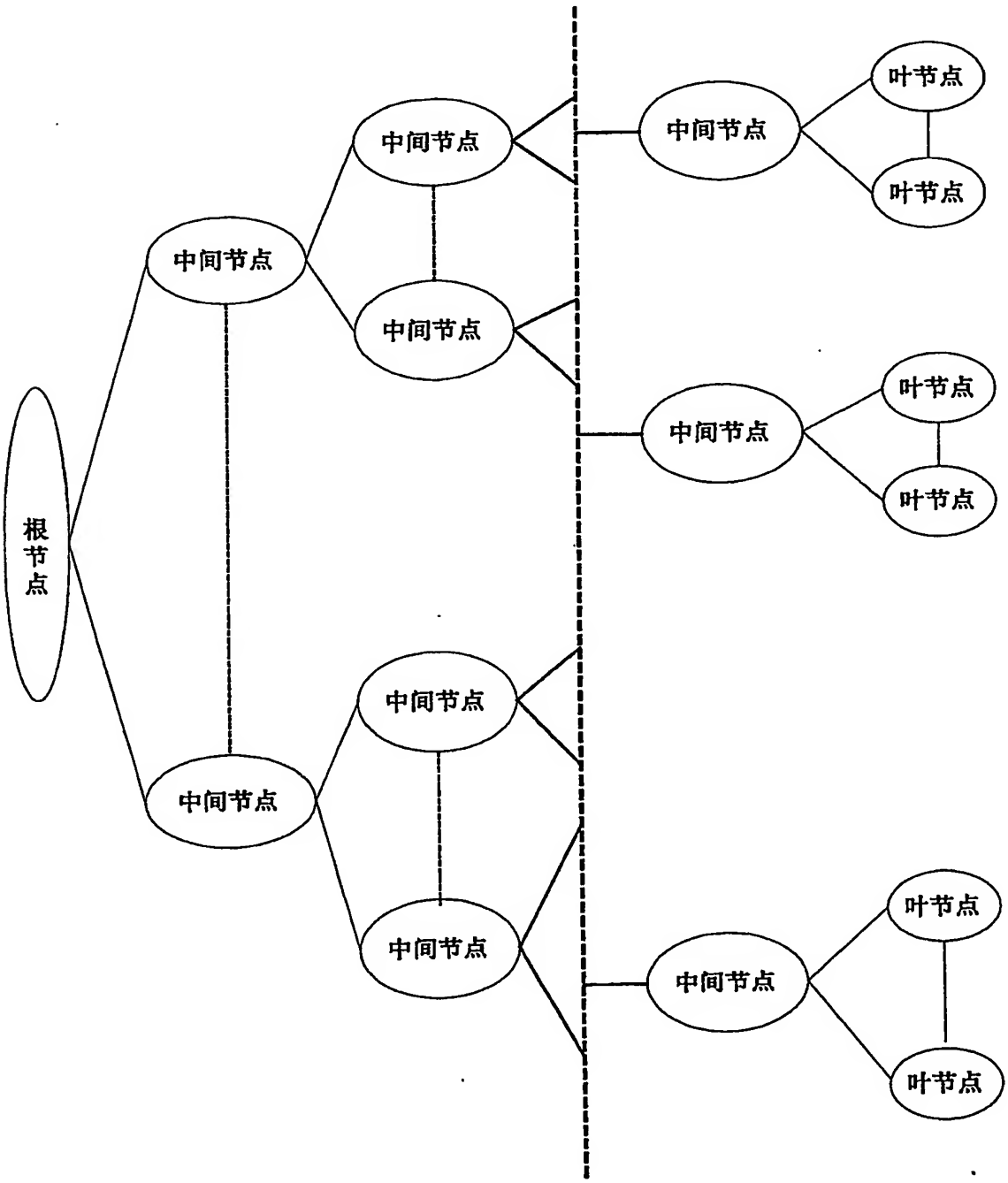

根节点
中间节点
中间节点
中间节点
中间节点
中间节点
中间节点
中间节点
中间节点
叶节点
叶节点
叶节点
叶节点
叶节点
叶节点

图 1

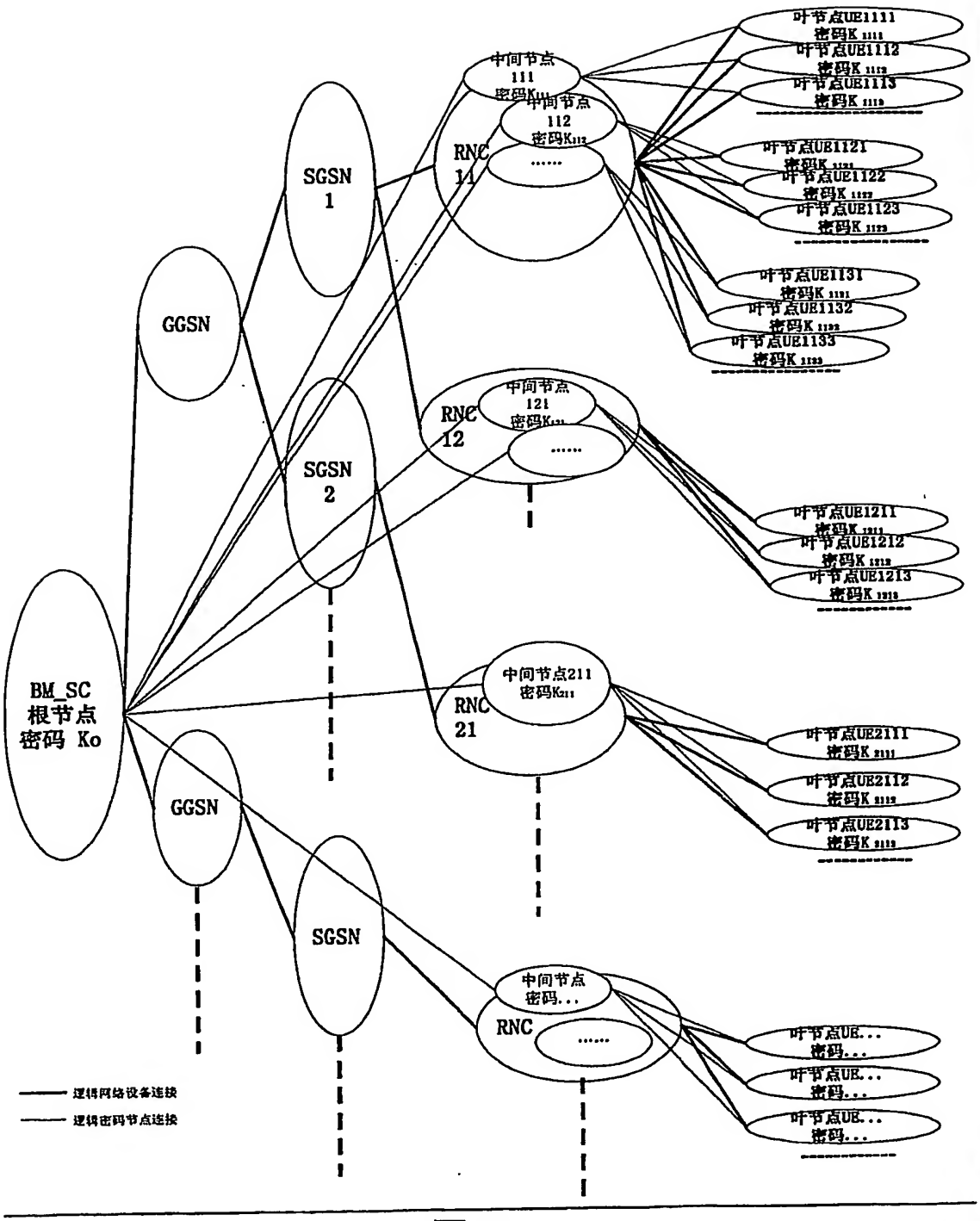

BM_SC
根节点
密码 Ko
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
RNC
12
RNC
21
RNC
中间节点
111
密码K111
中间节点
112
密码K112
.....
中间节点
121
密码K121
.....
中间节点211
密码K211
中间节点
密码...
.....
叶节点UE1111
密码K 1111
叶节点UE1112
密码K 1112
叶节点UE1113
密码K 1113
叶节点UE1121
密码K 1121
叶节点UE1122
密码K 1122
叶节点UE1123
密码K 1123
叶节点UE1131
密码K 1131
叶节点UE1132
密码K 1132
叶节点UE1133
密码K 1133
叶节点UE1211
密码K 1211
叶节点UE1212
密码K 1212
叶节点UE1213
密码K 1213
叶节点UE2111
密码K 2111
叶节点UE2112
密码K 2112
叶节点UE2113
密码K 2113
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
逻辑网络设备连接
逻辑密码节点连接

图 2

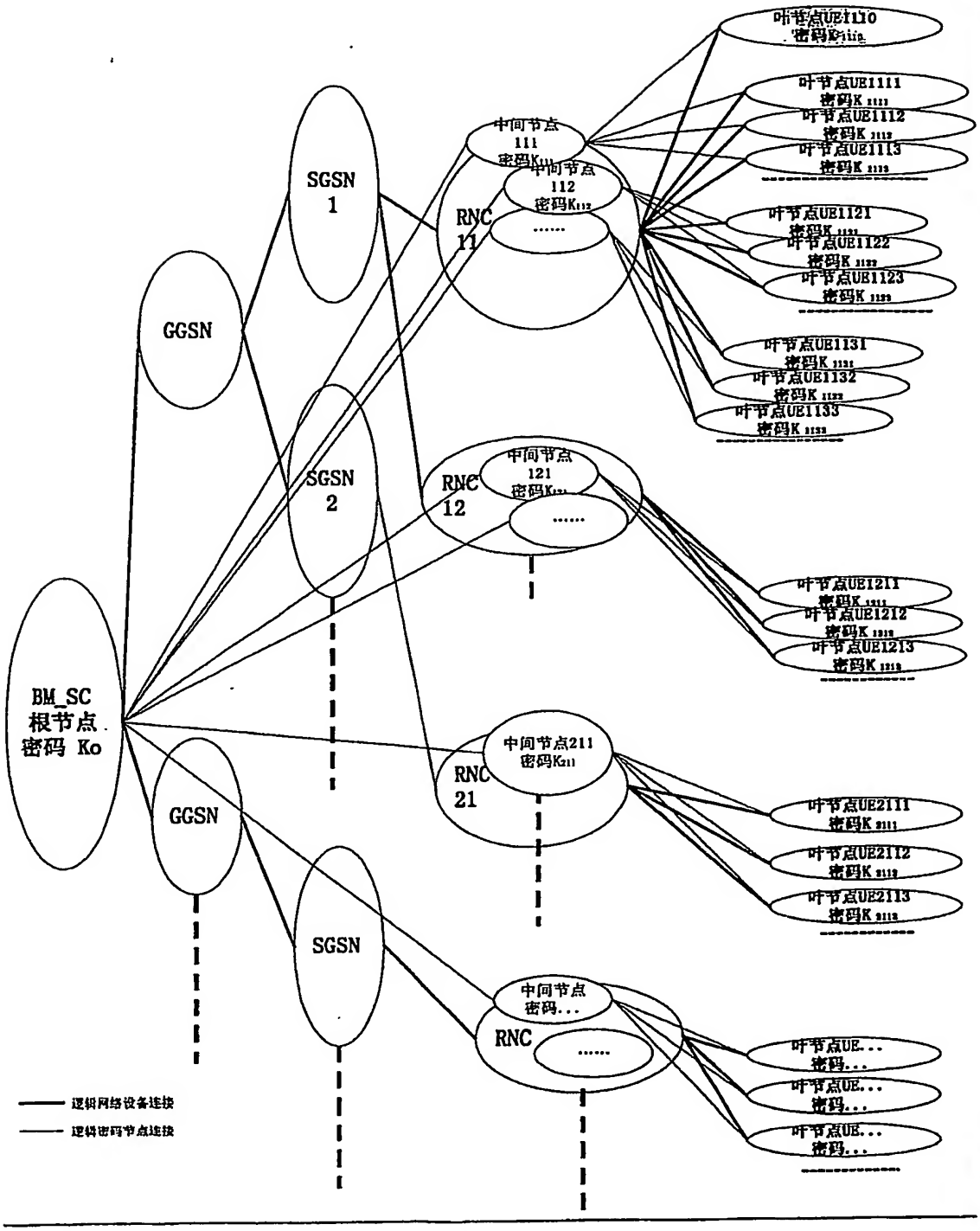

BM_SC
根节点
密码 Ko
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
RNC
12
RNC
21
RNC
中间节点
111
密码K111
中间节点
112
密码K112
.....
中间节点121
密码K121
.....
中间节点211
密码K211
中间节点
密码...
.....
叶节点UE1110
密码K1110
叶节点UE1111
密码K1111
叶节点UE1112
密码K1112
叶节点UE1113
密码K1113
叶节点UE1121
密码K1121
叶节点UE1122
密码K1122
叶节点UE1123
密码K1123
叶节点UE1131
密码K1131
叶节点UE1132
密码K1132
叶节点UE1133
密码K1133
叶节点UE1211
密码K1211
叶节点UE1212
密码K1212
叶节点UE1213
密码K1213
叶节点UE2111
密码K2111
叶节点UE2112
密码K2112
叶节点UE2113
密码K2113
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
逻辑网络设备连接
逻辑密码节点连接

图 3

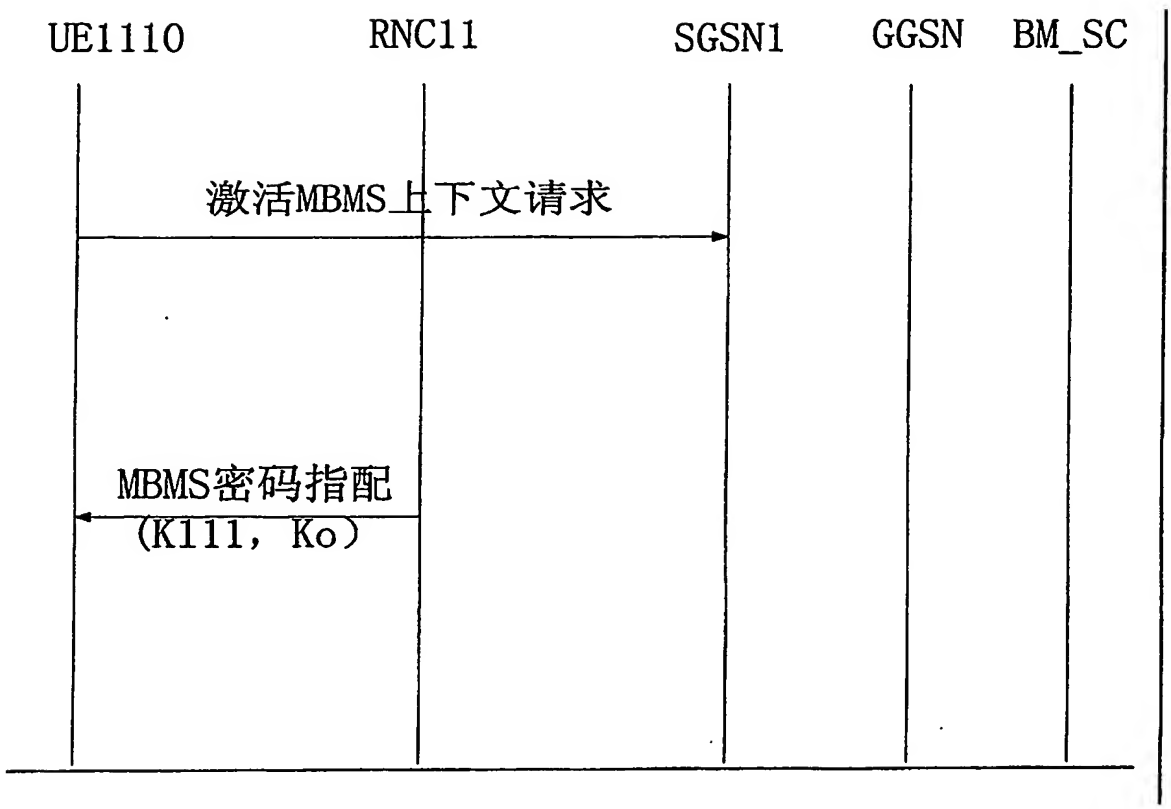


图 4

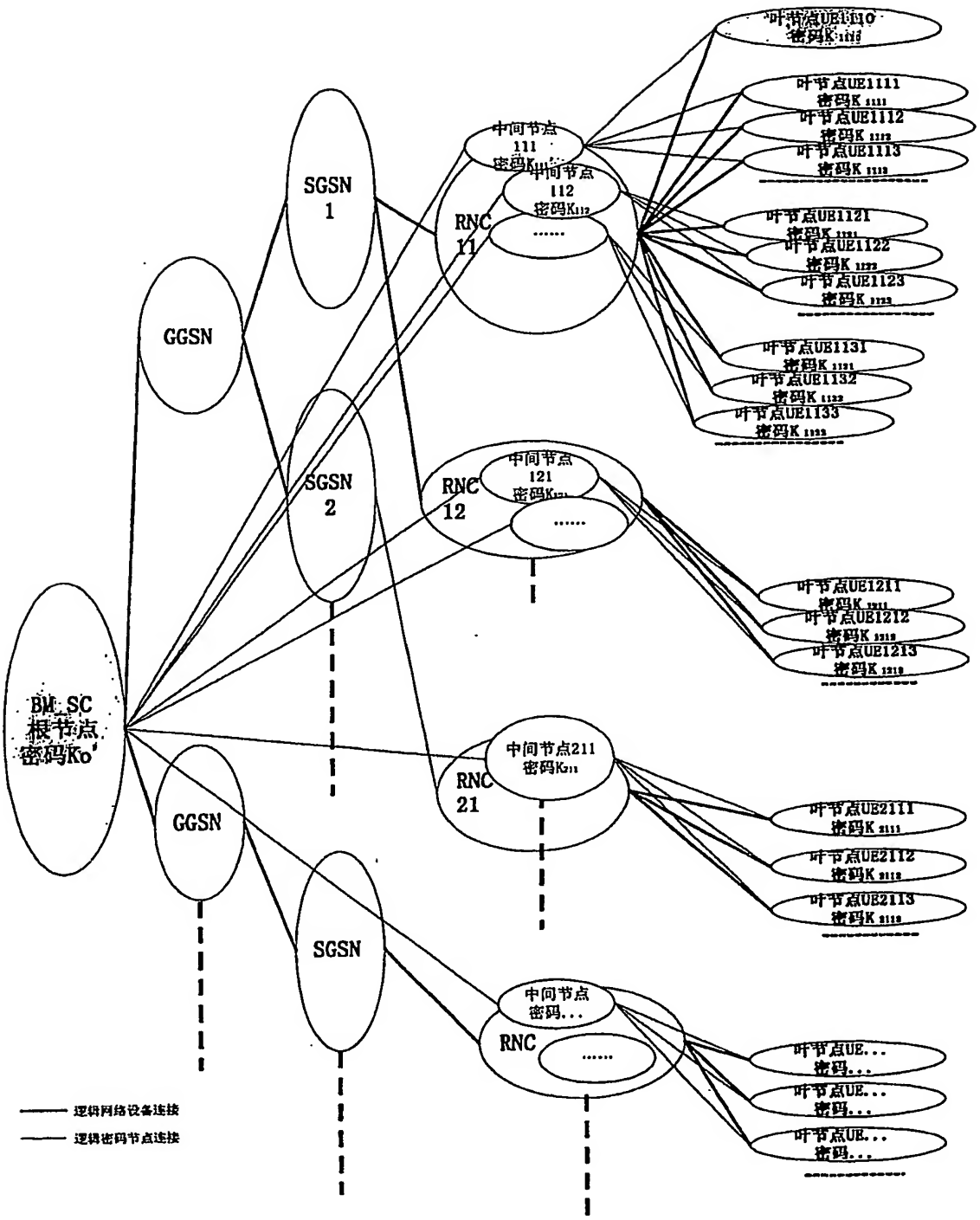

BM_SC
根节点
密码Ko
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
RNC
12
RNC
21
RNC
中间节点
111
密码K111
中间节点
112
密码K112
.....
中间节点
121
密码K121
.....
中间节点211
密码K211
中间节点
密码...
.....
叶节点UE1110
密码K1110
叶节点UE1111
密码K1111
叶节点UE1112
密码K1112
叶节点UE1113
密码K1113
叶节点UE1121
密码K1121
叶节点UE1122
密码K1122
叶节点UE1123
密码K1123
叶节点UE1131
密码K1131
叶节点UE1132
密码K1132
叶节点UE1133
密码K1133
叶节点UE1211
密码K1211
叶节点UE1212
密码K1212
叶节点UE1213
密码K1213
叶节点UE2111
密码K2111
叶节点UE2112
密码K2112
叶节点UE2113
密码K2113
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
逻辑网络设备连接
逻辑密码节点连接

图 5

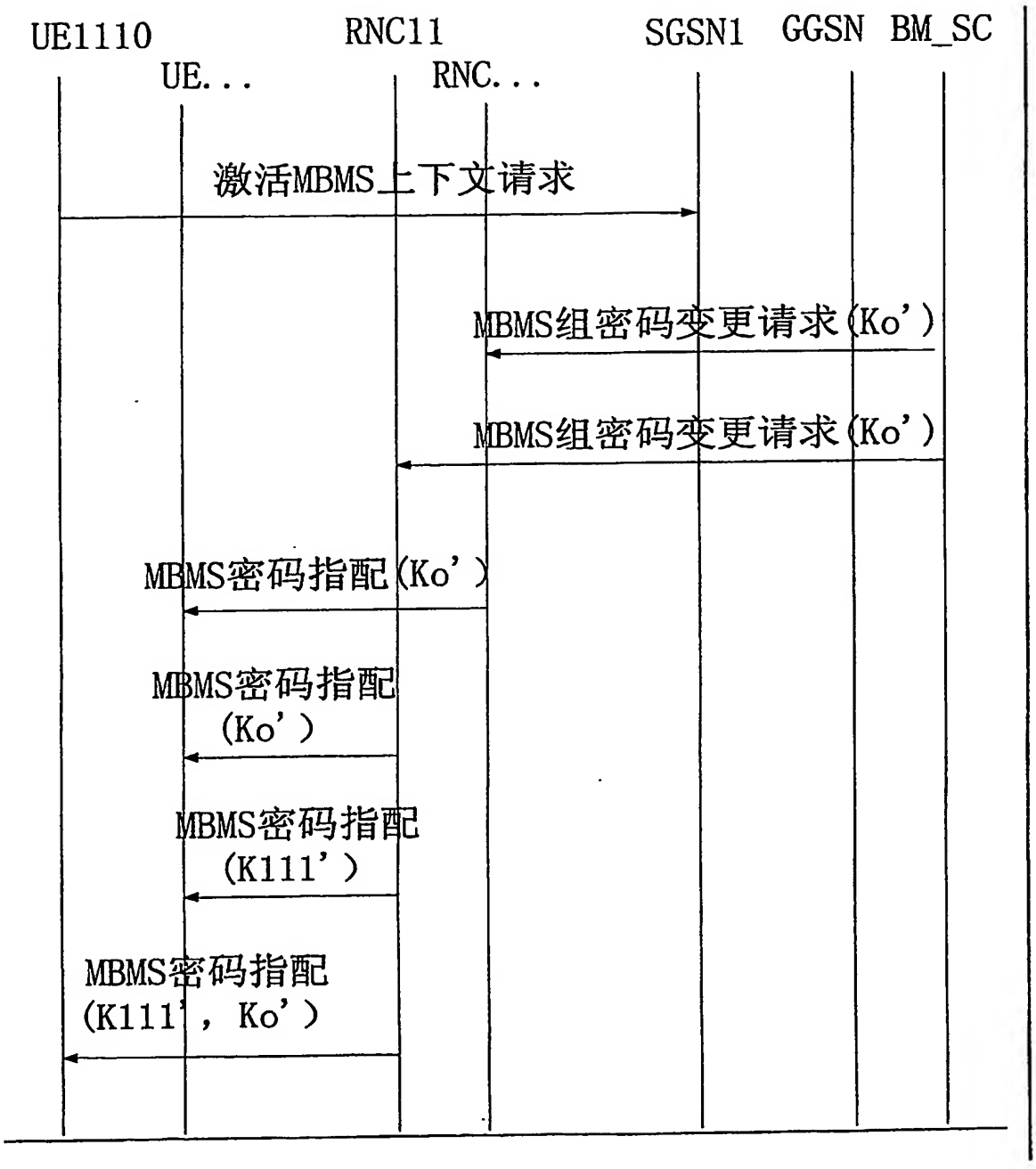

UE1110
UE...
RNC11
RNC...
SGSN1
GGSN
BM_SC
激活MBMS上下文请求
MBMS组密码变更请求(Ko')
MBMS组密码变更请求(Ko')
MBMS密码指配(Ko')
MBMS密码指配
(Ko')
MBMS密码指配
(K111')
MBMS密码指配
(K111', Ko')

图 6

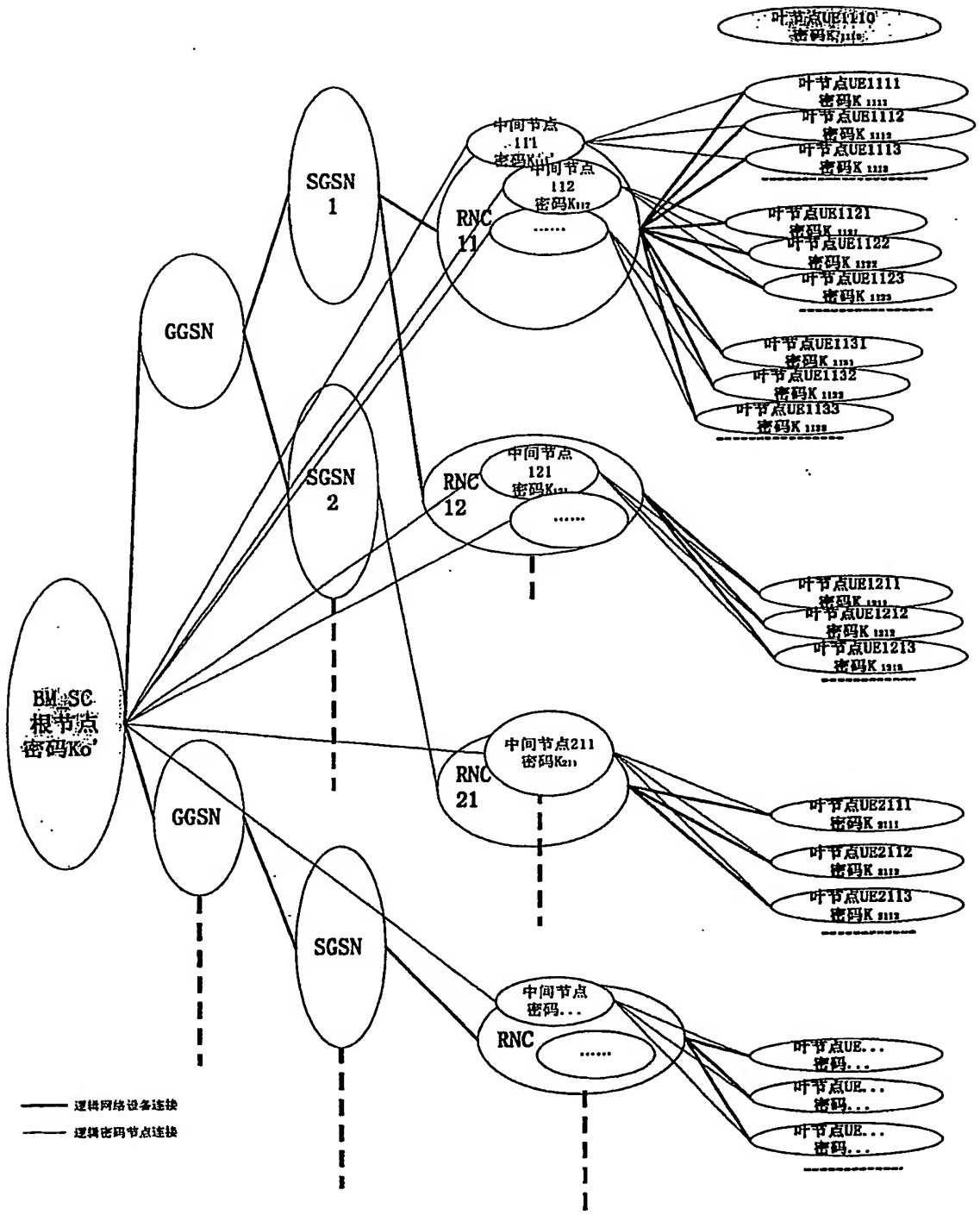

BM-SC
根节点
密码K0
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
RNC
12
RNC
21
RNC
中间节点
111
密码K111
中间节点
112
密码K112
.....
中间节点
121
密码K121
.....
中间节点211
密码K211
中间节点
密码...
.....
叶节点UE1110
密码K1110
叶节点UE1111
密码K1111
叶节点UE1112
密码K1112
叶节点UE1113
密码K1113
叶节点UE1121
密码K1121
叶节点UE1122
密码K1122
叶节点UE1123
密码K1123
叶节点UE1131
密码K1131
叶节点UE1132
密码K1132
叶节点UE1133
密码K1133
叶节点UE1211
密码K1211
叶节点UE1212
密码K1212
叶节点UE1213
密码K1213
叶节点UE2111
密码K2111
叶节点UE2112
密码K2112
叶节点UE2113
密码K2113
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
逻辑网络设备连接
逻辑密码节点连接

图 7

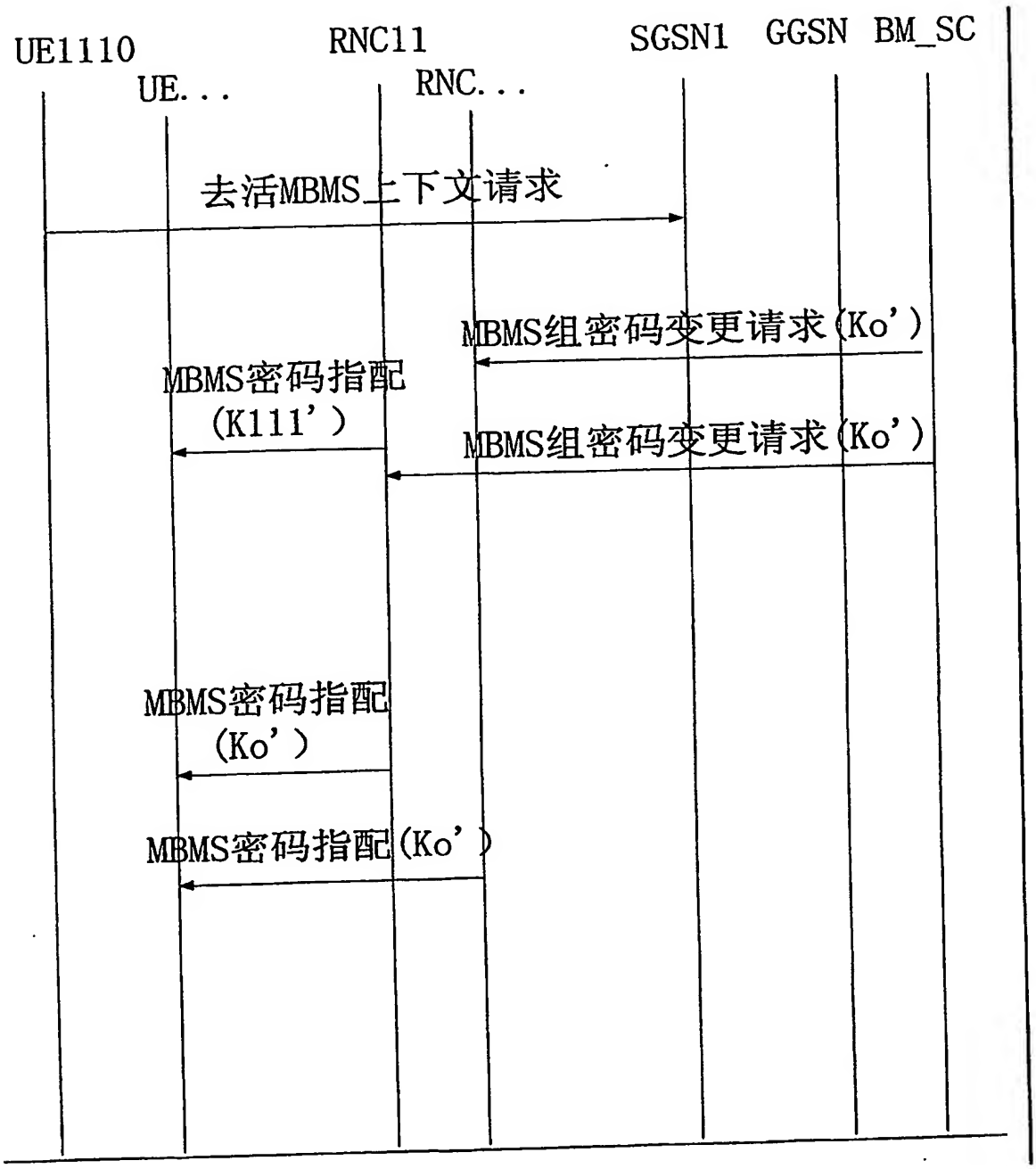

UE1110
UE...
RNC11
RNC...
SGSN1
GGSN
BM_SC
去活MBMS上下文请求
MBMS组密码变更请求(Ko')
MBMS密码指配
(K111')
MBMS组密码变更请求(Ko')
MBMS密码指配
(Ko')
MBMS密码指配(Ko')

图 8

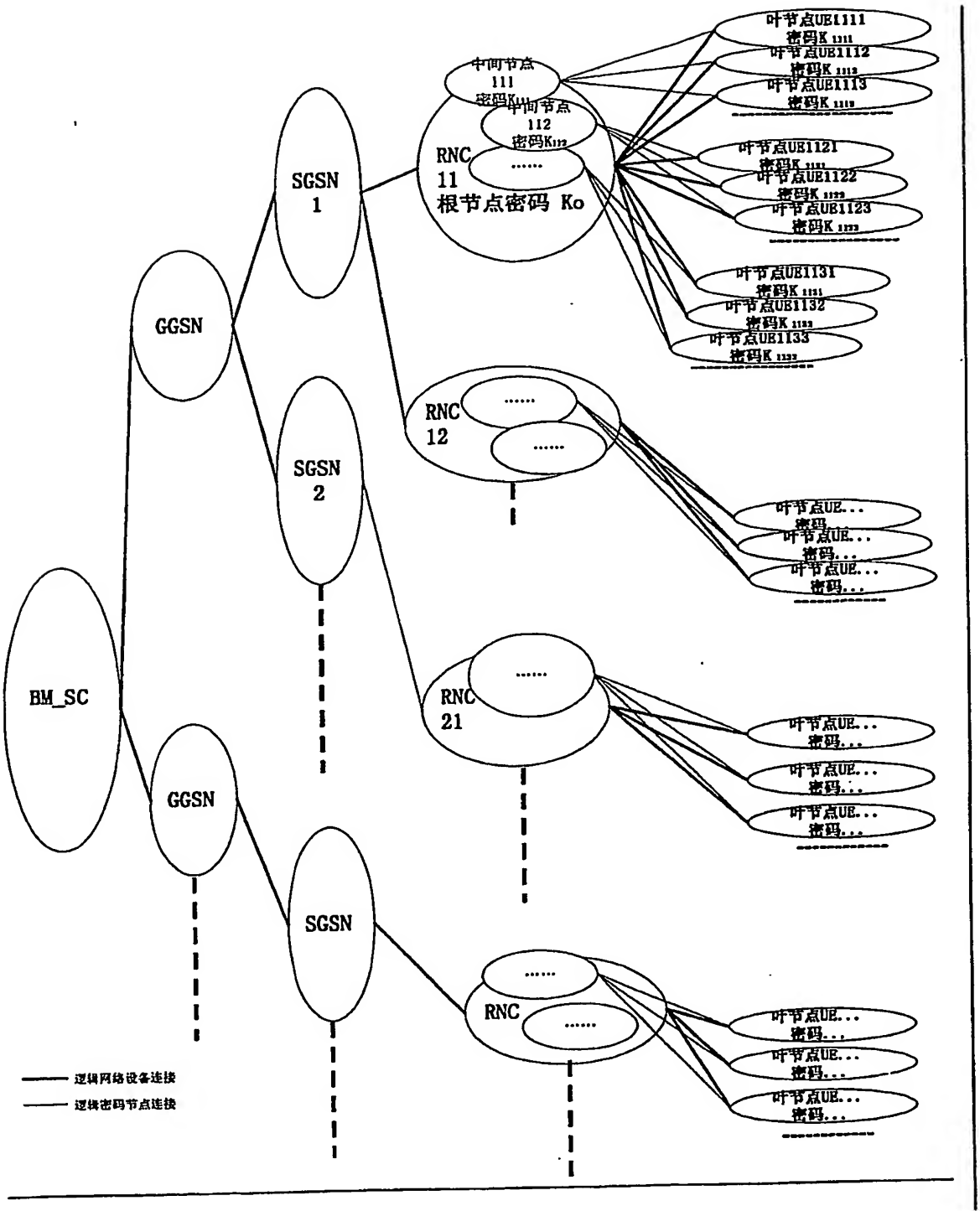

BM_SC
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
根节点密码 Ko
中间节点
111
密码K111
中间节点
112
密码K112
.....
叶节点UE1111
密码K 1111
叶节点UE1112
密码K 1112
叶节点UE1113
密码K 1113
叶节点UE1121
密码K 1121
叶节点UE1122
密码K 1122
叶节点UE1123
密码K 1123
叶节点UE1131
密码K 1131
叶节点UE1132
密码K 1132
叶节点UE1133
密码K 1133
RNC
12
.....
.....
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
RNC
21
.....
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
RNC
.....
.....
叶节点UE...
密码...
叶节点UE...
密码...
叶节点UE...
密码...
逻辑网络设备连接
逻辑密码节点连接

图 9

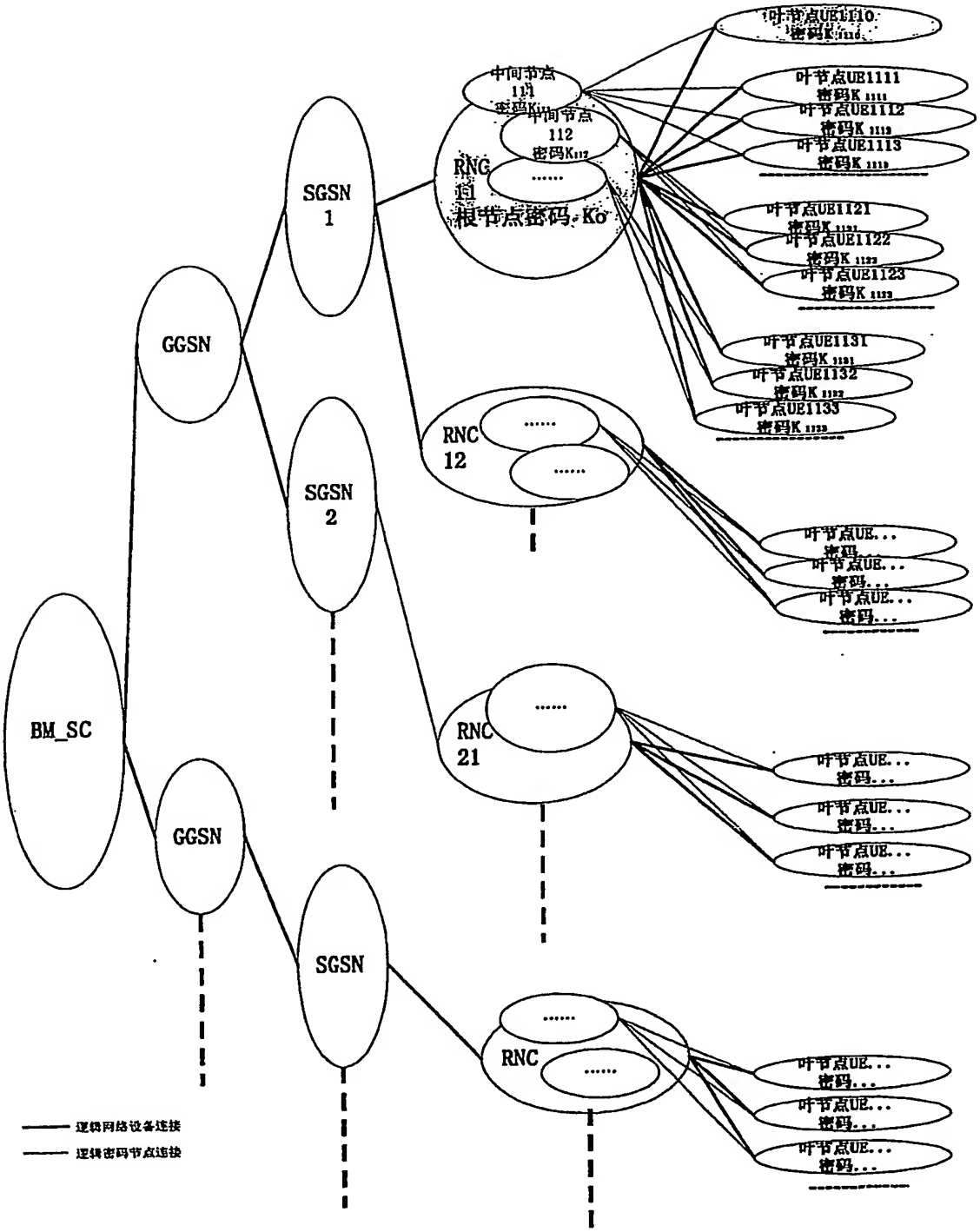

BM_SC
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
12
RNC
21
RNC
中间节点
111
密码K111
中间节点
112
密码K112
.....
根节点密码 Ko
叶节点UE1110
密码K1110
叶节点UE1111
密码K1111
叶节点UE1112
密码K1112
叶节点UE1113
密码K1113
叶节点UE1121
密码K1121
叶节点UE1122
密码K1122
叶节点UE1123
密码K1123
叶节点UE1131
密码K1131
叶节点UE1132
密码K1132
叶节点UE1133
密码K1133
叶节点UE...
密码...
逻辑网络设备连接
逻辑密码节点连接

图 10

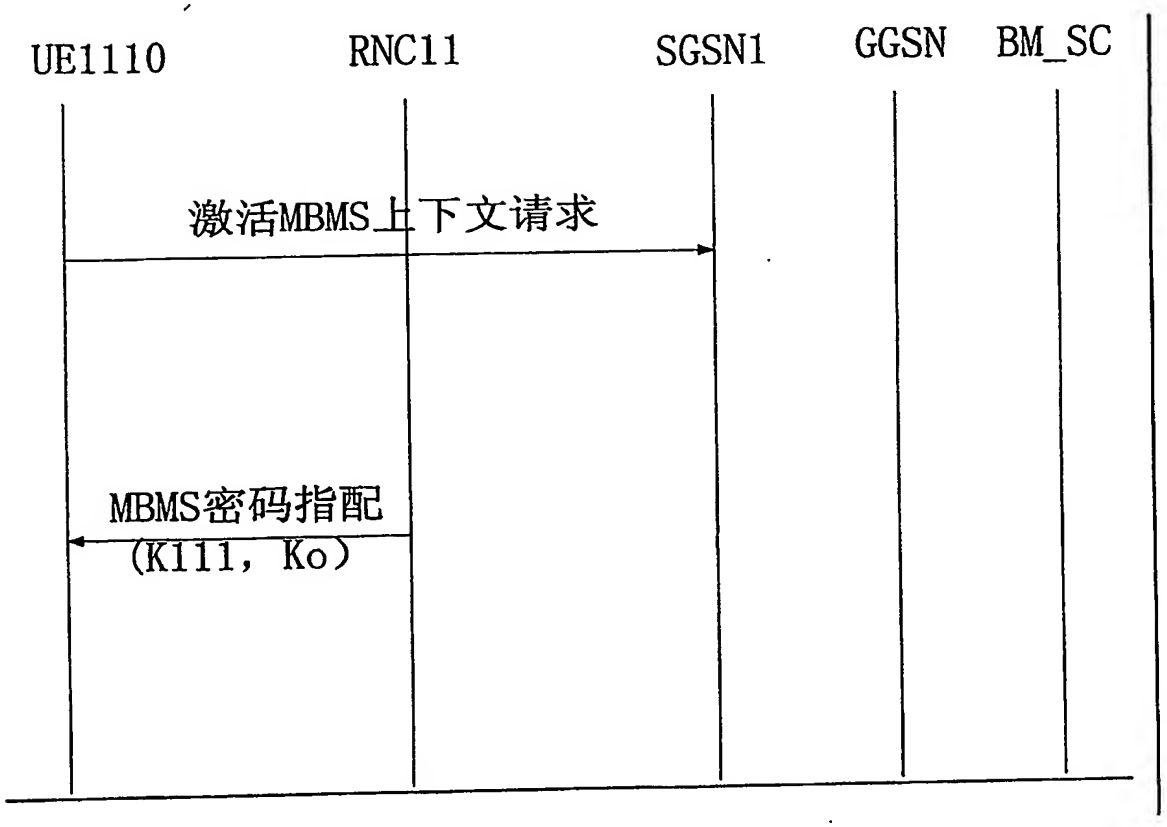


图 11

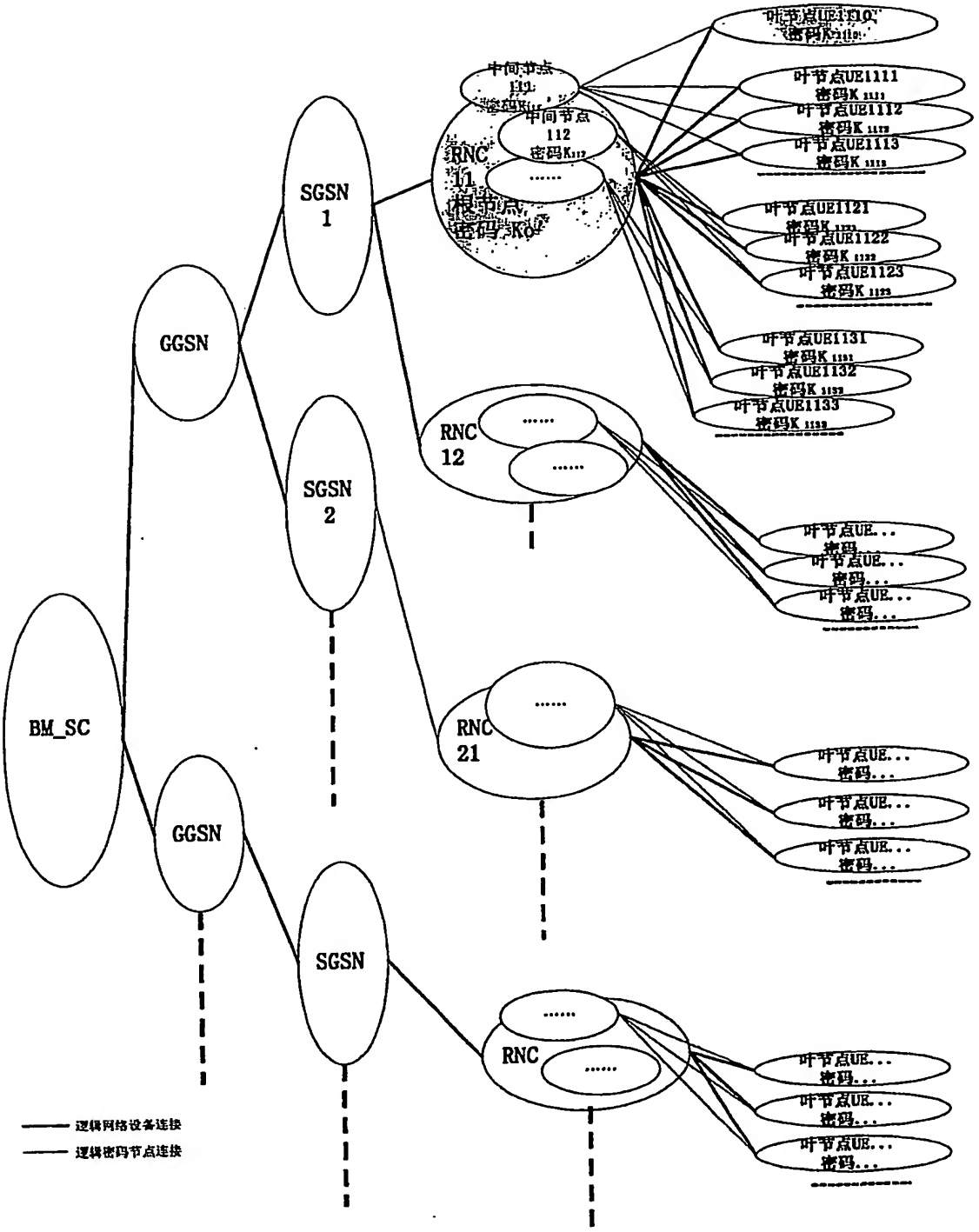

BM_SC
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
RNC
12
RNC
21
RNC
中间节点
111
中间节点
112
根节点
密码K0
叶节点UE1110
叶节点UE1111
叶节点UE1112
叶节点UE1113
叶节点UE1121
叶节点UE1122
叶节点UE1123
叶节点UE1131
叶节点UE1132
叶节点UE1133
逻辑网络设备连接
逻辑密码节点连接

图 12

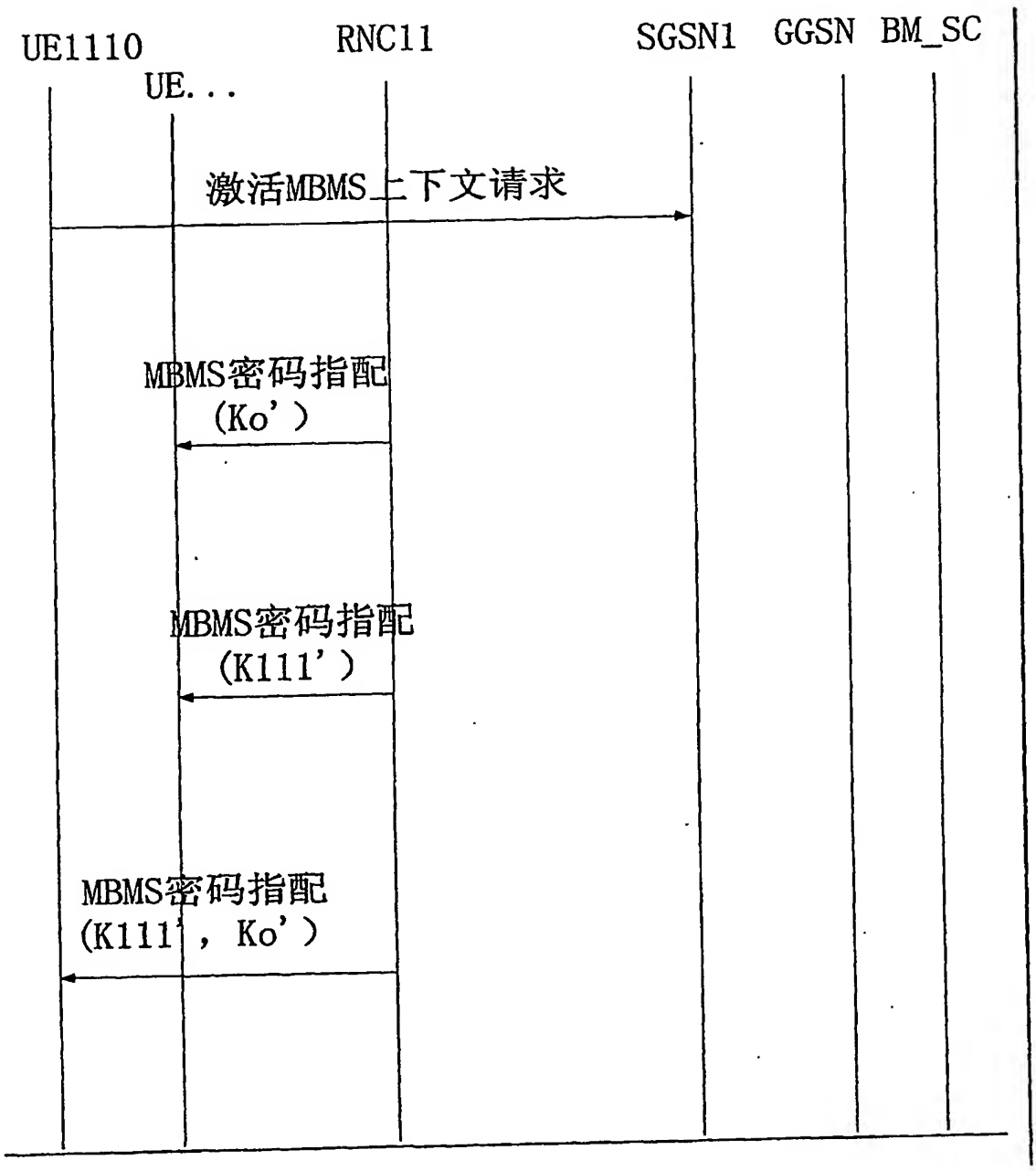

UE1110
UE...
RNC11
SGSN1
GGSN
BM_SC
激活MBMS上下文请求
MBMS密码指配
(Ko')
MBMS密码指配
(K111')
MBMS密码指配
(K111', Ko')

图 13

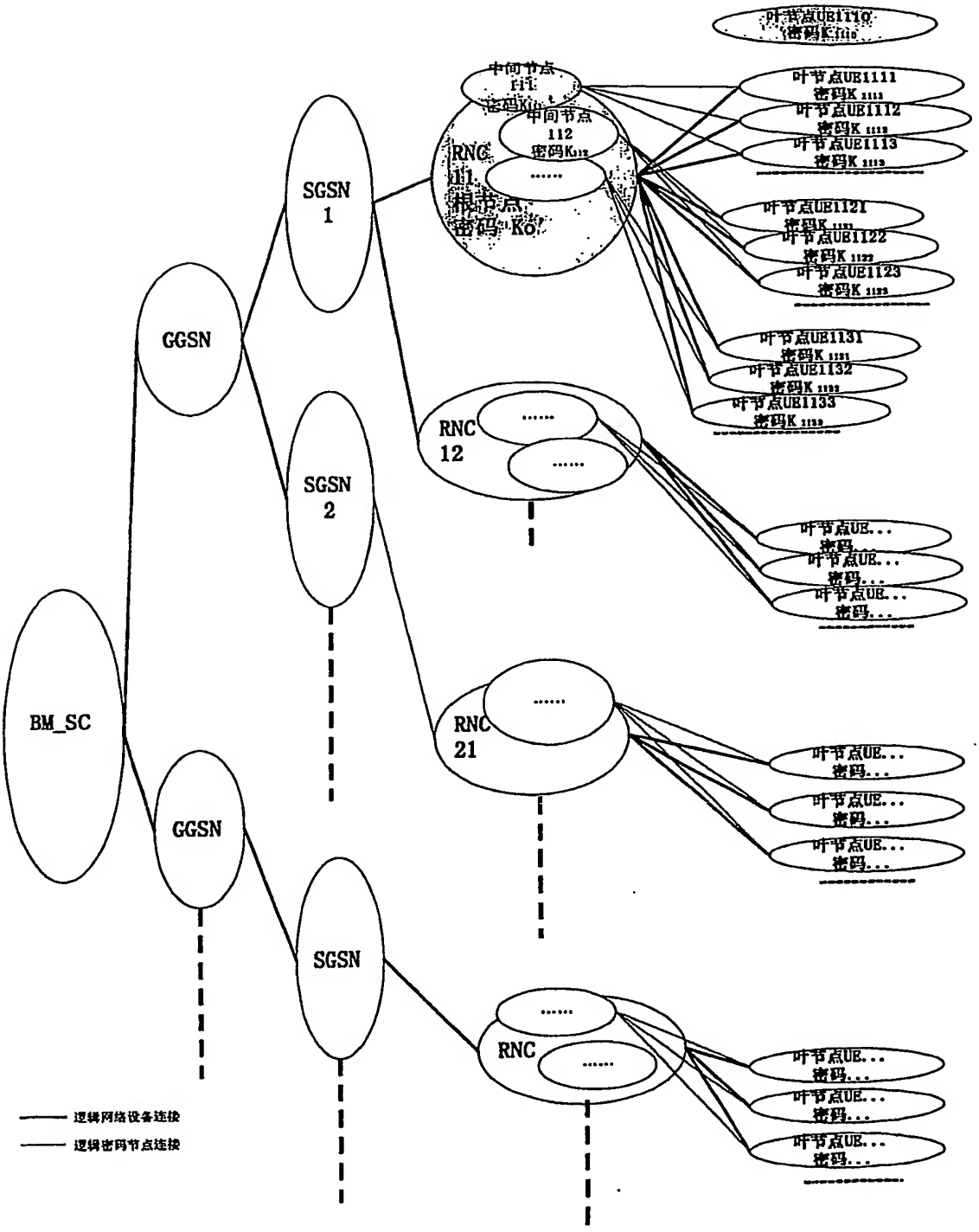

BM_SC
GGSN
GGSN
SGSN
1
SGSN
2
SGSN
RNC
11
RNC
12
RNC
21
RNC
中间节点
111
密码K111
中间节点
112
密码K112
根节点
密码 K0
叶节点UE1111
密码K 1111
叶节点UE1112
密码K 1112
叶节点UE1113
密码K 1113
叶节点UE1121
密码K 1121
叶节点UE1122
密码K 1122
叶节点UE1123
密码K 1123
叶节点UE1131
密码K 1131
叶节点UE1132
密码K 1132
叶节点UE1133
密码K 1133
逻辑网络设备连接
逻辑密码节点连接

图 14

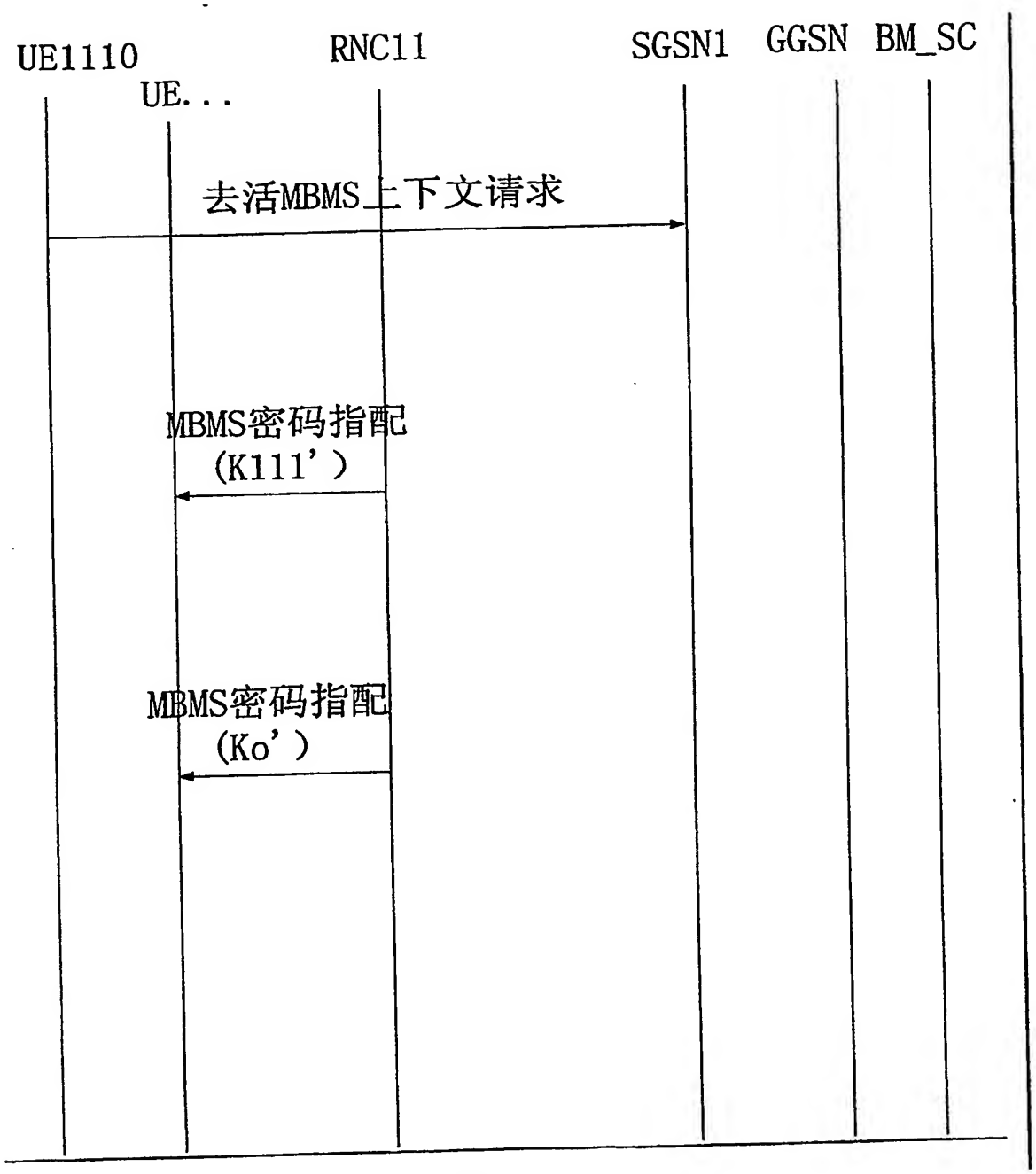

UE1110
UE...
RNC11
SGSN1
GGSN
BM_SC
去活MBMS上下文请求
MBMS密码指配
(K111')
MBMS密码指配
(Ko')

图 15

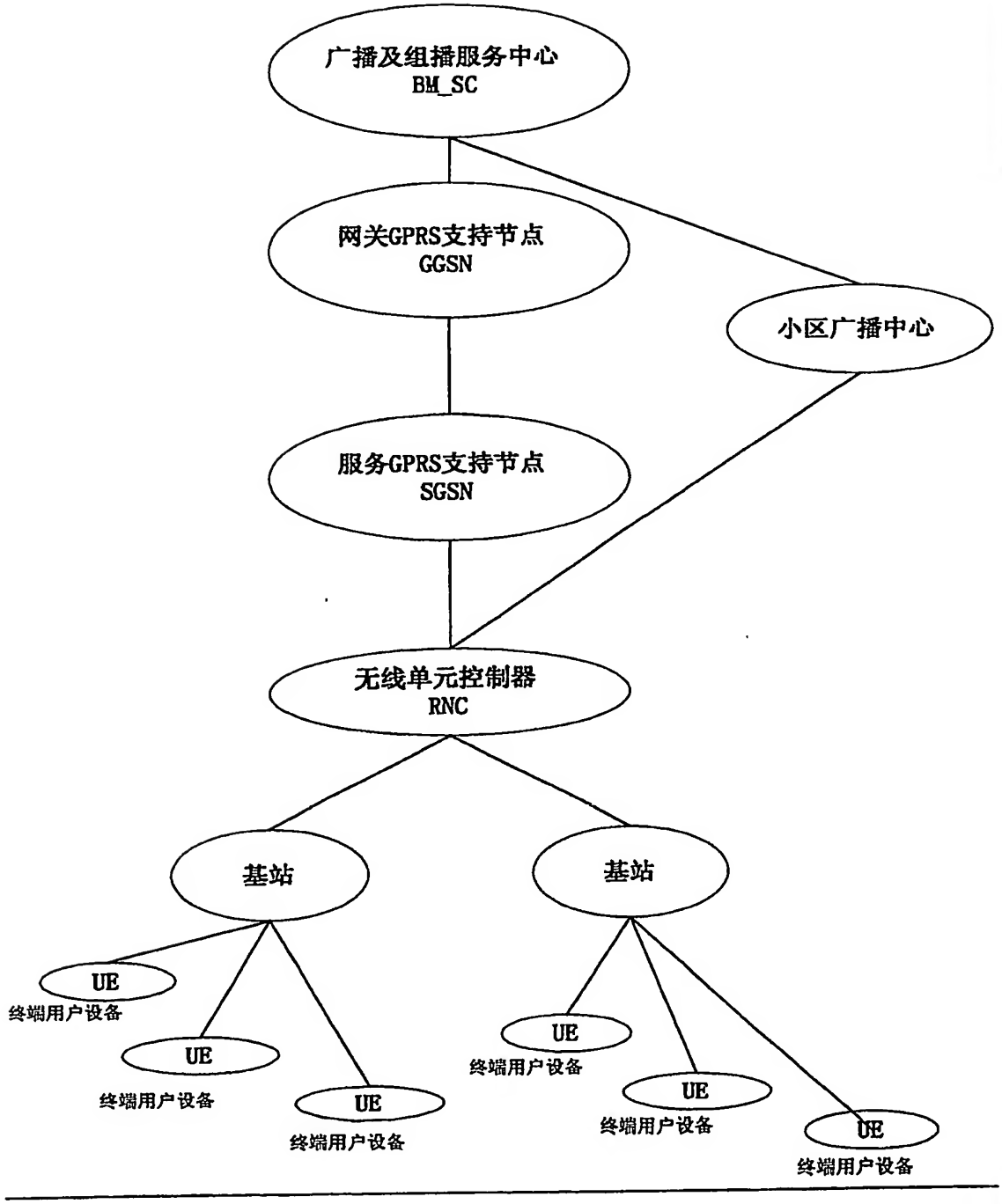

广播及组播服务中心
BM_SC
网关GPRS支持节点
GGSN
小区广播中心
服务GPRS支持节点
SGSN
无线单元控制器
RNC
基站
基站
UE
终端用户设备
UE
终端用户设备
UE
终端用户设备
UE
终端用户设备
UE
终端用户设备
UE
终端用户设备

图 16

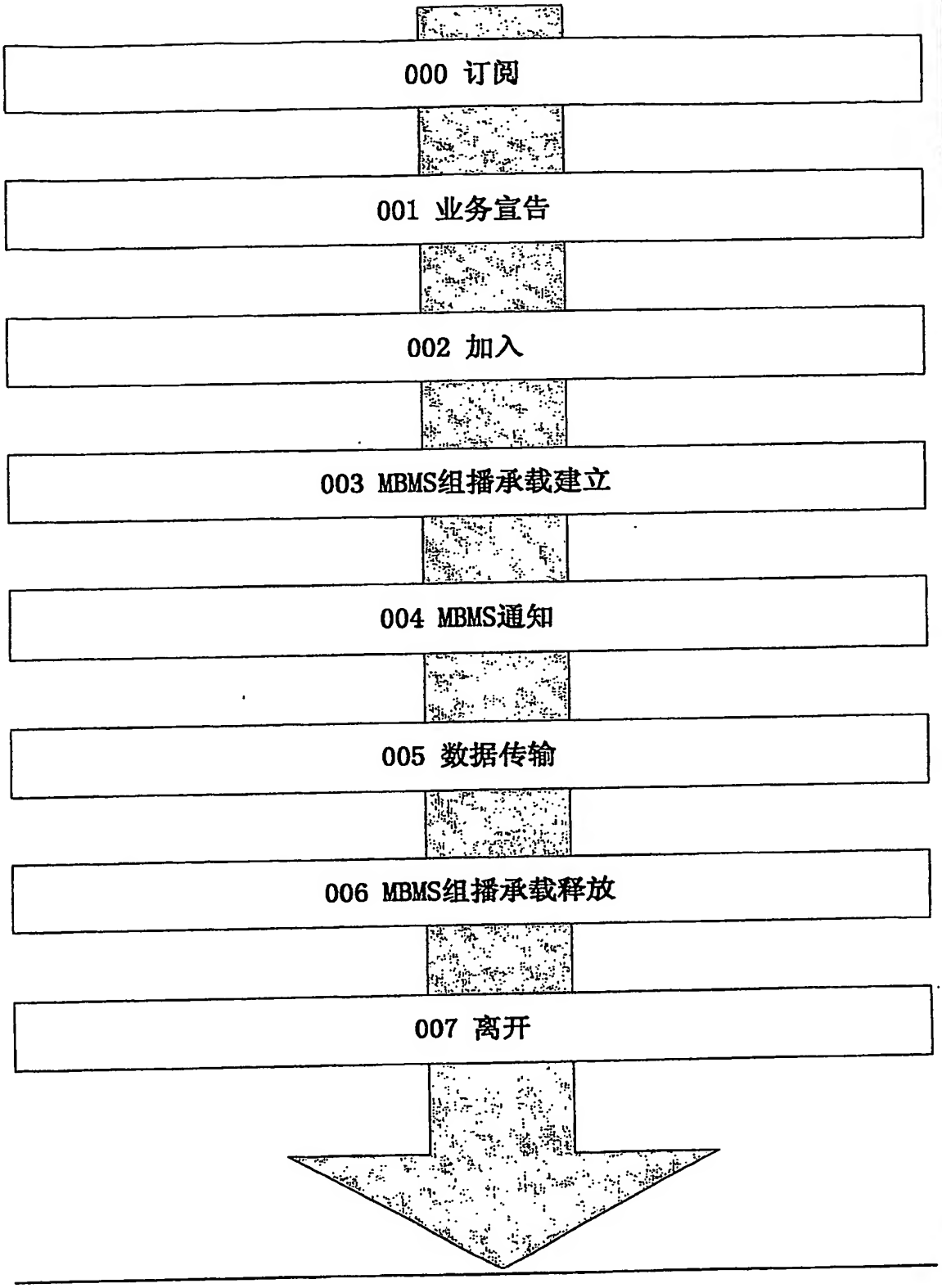

000 订阅
001 业务宣告
002 加入
003 MBMS组播承载建立
004 MBMS通知
005 数据传输
006 MBMS组播承载释放
007 离开

图 17